Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1   1 (Currently Amended). A method of protecting a ~~document~~ check, which

2   will be transformed into a value bearing instrument after adding additional

3   markings to the ~~document~~ check, from fraudulent alteration of the

4   markings comprising the steps of:

5   generating encryptions of a unique identifier X of the document,

6   the unique identifier X being check data including a bank ID, an account

7   ID number and a check number printed on the ~~document~~ check, the

8   encryptions being $Sign_{k,0}(X)$, where $Sign_{k,0}(X)$ is a cryptographic function

9   or family thereof which is known only to an institution which issues the

10   check, $Sign_{k,0}(X)$ being used to authenticate the check; and

11   covering each critical field k, k=1,2,3..., of the ~~document~~ check

12   where markings are to be added with ~~encrypted versions of X $Sign_{k,0}(X)$,~~

13   ~~where $Sign_{k,0}(X)$ is a family of cryptographic functions which is known~~

14   ~~only to an institution which issues the document, $Sign_{k,0}(X)$ being used to~~

15   ~~authenticate the document~~ a large number of lines of fine print, the lines of

16   fine print comprising the cryptographic function $Sign_k$, the critical fields k

17   including a date field, a payee field, amount fields, a payer's signature

18   field, and an endorser's field.

2 (Canceled).

1   3 (Currently Amended). The method of protecting a ~~document~~ check from

2   fraudulent alteration recited in claim ~~2~~ 1, wherein each critical field k of

3   the document, in addition to being covered by the encrypted version of X,

4      $Sign_{k,0}(X)$, is covered with another encrypted version of X, $Sign_k(X)$,

5   where $Sign_k(X)$ is another cryptographic function or family thereof

6   different from the cryptographic function $Sign_{k,0}(X)$ which is known to a

7   larger number of authorized institutions for performing an initial

8   authentication of the ~~document~~ <u>check</u>.

4 (Canceled).

1   5 (Currently Amended). The method of protecting a ~~document~~ <u>check</u> from

2   fraudulent alteration recited in claim 3, wherein each critical field k of the

3   ~~document~~ <u>check</u>, in addition to being covered by encrypted versions of X,

4      $Sign_k(X)$ and $Sign_{k,0}(X)$, is covered with a third encrypted version of X,

5      $Sec_k(X)$, where $Sec_k(X)$ is another cryptographic function or family thereof

6   different from the cryptographic functions $Sign_{k,0}(X)$ and $Sign_k(X)$ which is

7   known to a small group within the institution which issues the ~~document~~

8   <u>check</u> for performing final authentication of the ~~document~~ <u>check</u>.

1   6 (Currently Amended). The method of protecting a ~~document~~ <u>check</u> from

2   fraudulent alteration recited in claim 5, further comprising the step of

3   indexing the cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k by a number

4   corresponding to the field k, so that each line comprises different

5   encryptions of X such that each cryptographic function $Sign_k(X)$,

6      $Sign_{k,0}(X)$ and $Sec_k(X)$ is a family of different cryptographic functions.

1   7 (Currently Amended). The method of protecting a ~~document~~ <u>check</u> from

2   fraudulent alteration recited in claim 6, wherein the families of

3   cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k prevent cryptographic

4   functions which have been obscured at different places by marks added to

5   the ~~document~~ <u>check</u> from being used to reconstitute the full cryptographic

6   function.

1   8 (Currently Amended). The method of protecting a ~~document~~ <u>check</u> from

2   fraudulent alteration recited in claim 1, wherein electronic deposit of a

3   ~~document~~ <u>check</u> transformed into a value bearing instrument comprises the

4   steps of:

5   scanning the ~~document~~ <u>check</u> with a scanner to generate a digitized

6   version of the ~~document~~ check ; and

7   transmitting the digitized version of the ~~document~~ check for

8   deposit.

1   9 (Currently Amended). The method of protecting a ~~document~~ check from

2   fraudulent alteration recited in claim 8, wherein electronic deposit of a

3   ~~document~~ check transformed into a value bearing instrument further

4   comprises the step of endorsing the ~~document~~ check, if needed, having

5   printed thereon encryptions in at least selected locations where markings

6   are added to transform the ~~document~~ check into a value bearing

7   instrument, the act of endorsing obscuring some of the encryptions.

1   10 (Currently Amended).The method of protecting a ~~document~~ check from

2   fraudulent alteration recited in claim ~~8~~ 5, wherein electronic deposit of a

3   ~~document~~ transformed into a value bearing instrument further comprises

4   the steps of:

5   generating a digitized version of the check in at least selected

6   locations where markings are added to transform the check into a value

7   bearing instrument;

8   extracting from the digitized version of the ~~document~~ check the

9   unique identifier X and a corresponding digital encryption of X, $Sign_k(X)$,

10   which is known to a large number of authorized institutions; and

11   comparing a decrypted version of $Sign_k(X)$ to the unique identifier

12   X as an initial authentication of the ~~document~~ check.

1   11 (Currently Amended). The method of protecting a ~~document~~ check

2   from fraudulent alteration recited in claim 10, wherein electronic deposit

3   of a document transformed into a value bearing instrument further

4   comprises the steps of:

5   extracting from the digitized version of the ~~document~~ check the

6   unique identifier X and a corresponding digital encryption of X, $Sign_{k,0}(X)$,

7   which is known only to an institution that issues the ~~document~~ check; and

8 comparing a decrypted version of $Sign_{k,0}(X)$ to the unique identifier
9 X as a further authentication of the ~~document~~ check.

1 12 (Currently Amended). The method of protecting a ~~document~~ check
2 from fraudulent alteration recited in claim 11, wherein electronic deposit
3 of a document transformed into a value bearing instrument further
4 comprises the steps of:
5   extracting from the digitized version of the ~~document~~ check the
6 unique identifier X and a corresponding digital encryption of X, $Sec_k(X)$,
7 which is known to a small group within the institution that issues the
8 ~~document~~ check; and
9   comparing a decrypted version of $Sec_k(X)$ to the unique identifier X
10 as a final authentication of the ~~document~~ check.

1 13 (Currently Amended). The method of protecting a ~~document~~ check
2 from fraudulent alteration recited in claim 1, wherein portions of the lines
3 of fine print are obscured by writing added to the ~~document~~ check when
4 transforming the ~~document~~ check into a value bearing instrument.

  14 (Canceled).

1 15 (Currently Amended). The method of protecting a ~~document~~ check
2 from fraudulent alteration recited in claim ~~14~~ 1, wherein an issuing bank
3 chooses a first secret key $Sign_k$ using a secure cryptographic generator
4 (SCG), further comprising the steps of:
5   computing ~~a~~ the first family of encrypted functions $Sign_k(X)$; and
6   communicating the key $Sign_k$ to banks and other authorized
7 institutions involved in depositing of checks, the family of encrypted
8 functions $Sign_k(X)$ allowing the payee's bank to perform a first
9 authentication of the check.

1 16 (Currently Amended). The method of protecting a ~~document~~ check

2 from fraudulent alteration recited in claim 15, wherein an issuing bank

3 chooses a second secret key $Sign_{k,0}$ using a SCG, further comprising the

4 steps of:

5   computing ~~a~~ the second family of encrypted functions $Sign_{k,0}(X)$,

6 key $Sign_{k,0}$ remaining the exclusive property of the issuing bank; and

7   using SCGs, communicating the key $Sign_{k,0}$ to all branches of the

8 issuing bank where check clearing is done, the family of encrypted

9 functions $Sign_{k,0}(X)$ being used exclusively by the issuing bank and

10 branches involved in the clearing of checks.

1 17 (Currently Amended). The method of protecting a ~~document~~ check

2 from fraudulent alteration recited in claim 16, wherein an issuing bank

3 chooses a third secret key Sec_k which is exclusively known to a small

4 group within the issuing bank, further comprising the step of computing ~~a~~

5 the third family of encrypted functions $Sec_k(X)$, the secret key Sec_k being

6 used by the issuing bank as final instrument to verify the check.

1 18 (Currently Amended). The method of protecting a ~~document~~ check

2 from fraudulent alteration recited in claim ~~14~~ 1, wherein the check is

3 deposited by a payee electronically from a location remote from a bank or

4 Automatic Teller Machine (ATM) .

1 19 (Currently Amended). The method of protecting a ~~document~~ check

2 from fraudulent alteration recited in claim ~~14~~ 5, wherein electronic deposit

3 of the check by a payee comprises the steps of:

4   endorsing the check having printed thereon encryptions in at least

5 selected locations where information is written by a payer, the act of

6 endorsing by the payee obscuring some of the encryptions;

7   scanning the endorsed check with a scanner to generate a digitized

8 version of the check;

9   transmitting the digitized version of the check for deposit to the

10   payee's bank.

1   20 (Currently Amended).The method of protecting a ~~document~~ check from

2   fraudulent alteration recited in claim 19, wherein electronic deposit of the

3   check by a payee comprises the steps of:

4   extracting by the payee's bank from the digitized version of the

5   check the unique identifier X and a corresponding digital encryption of X,

6      $Sign_k(X)$, which is known to a large number of authorized institutions

7   including the payee's bank; and

8   comparing by the payee's bank a decrypted version of $Sign_k(X)$ to

9   the unique identifier X as an initial authentication of the check.

1   21 (Currently Amended). The method of protecting a ~~document~~ check

2   from fraudulent alteration recited in claim 20, wherein electronic deposit

3   of the check further comprises the steps of:

4   extracting from the digitized version of the check the unique

5   identifier X and a corresponding digital encryption of X, $Sign_{k,0}(X)$, which

6   is known only to a bank that issues the check; and

7   comparing by the payor's bank a decrypted version of $Sign_{k,0}(X)$ to

8   the unique identifier X as a further authentication of the check.

1   22 (Currently Amended). The method of protecting a ~~document~~ check

2   from fraudulent alteration recited in claim 21, wherein electronic deposit

3   of the check further comprises the steps of:

4   extracting from the digitized version of the check the unique

5   identifier X and a corresponding digital encryption of X, $Sec_k(X)$, which is

6   known to a small group within the bank that issues the check; and

7   comparing a decrypted version of $Sec_k(X)$ to the unique identifier X

8   as a final authentication of the check.

1   23 (Currently Amended). The method of protecting a ~~document~~ check

2   from fraudulent alteration recited in claim 19, further comprising the step

3   of accessing a database by the payee's bank where the unique identifier X

4   and first encrypted function $Sign_k(X)$ is registered to determine whether the

5   check has been previously presented for deposit.

1   24 (Currently Amended). The method of protecting a ~~document~~ check

2   from fraudulent alteration recited in claim 19, further comprising the step

3   of registering a check to be deposited by the payee with ~~an~~ a secure

4   cryptgraphic generator (SCG) to prevent multiple deposits.

1   25 (Currently Amended). A ~~document~~ check protecting against fraudulent

2   alteration of markings added to the ~~document~~ check to transform the

3   ~~document~~ check into a value bearing instrument, the ~~document~~ check

4   having printed thereon a unique identifier X, the unique identifier

5   including a bank ID, an account ID number and a check number, the check

6   further having critical fields k, k=1,2,3..., the critical fields including a date

7   field, a payee field, amount fields, a payer's field, and an endorser's field,

8   and ~~covering~~ each critical field k, k=1,2,3..., being covered a large number

9   of lines of fine print comprising ~~where markings are added to the~~

10   ~~document~~ encrypted versions ~~a~~ the unique identifier X printed on the

11   document, $Sign_{k0}(X)$, where $Sign_{k0}(X)$ is a cryptographic function or family

12   thereof which is known only to an institution which issues the document,

13      $Sign_{k0}(X)$ being used to authenticate the document.

26 (Canceled).

1   27 (Currently Amended). The ~~document~~ check recited in claim ~~26~~ 25,

2   wherein each critical field k of the ~~document~~ check, in addition to being

3   covered by encrypted versions of X, $Sign_{k0}(X)$, is covered with another

4   encrypted version of X, $Sign_k(X)$, where $Sign_k(X)$ is another cryptographic

5   function or family thereof different from the cryptographic function

6        $Sign_{k,0}(X)$ which is known to a larger number of authorized institutions for

7   performing an initial authentication of the document.

1   28 (Currently Amended). The ~~document~~ <u>check</u> recited in claim 27, wherein

2   each critical field k of the ~~document~~ <u>check</u>, in addition to being covered by

3   encrypted versions of X, $Sign_{k,0}(X)$ and $Sign_k(X)$, is covered with a third

4   encrypted version of X, $Sec_k(X)$ is another cryptographic function or

5   family thereof different from the cryptographic functions $Sign_{k,0}(X)$ and

6      $Sign_k(X)$ which is known to a small group within the institution which

7   issues the document for performing final authentication of the document.

1   29 (Currently Amended). The ~~document~~ <u>check</u> recited in claim 28, wherein

2   the cryptographic functions $Sign_k$, $Sign_{k,0}$ and Sec_k, are indexed by a

3   number corresponding to the field k, so that each line comprises different

4   encryptions of X such that each cryptographic function $Sign_k(X)$,

5      $Sign_{k,0}(X)$, $Sec_k(X)$ is a family of different cryptographic functions.

6   30 (Currently Amended). The ~~document~~ <u>check</u> recited in claim 29, wherein

7   the act of adding markings to the ~~document~~ <u>check</u> to transform the

8   ~~document~~ <u>check</u> into a value bearing instrument obscures some of the

9   encryptions, the families of different cryptographic functions preventing

10   cryptographic functions which have been obscured at different places from

11   being used to reconstitute the full cryptographic function.

     31 (Canceled).

1   32 (Currently Amended). The ~~document~~ <u>check</u> recited in claim ~~31~~ <u>25</u>,

2   wherein the act of adding markings to the check to transform the document

3   into a value bearing instrument obscures some of the encryptions

     33 (Canceled).

1   34 (Currently Amended). The ~~document~~ <u>check</u> recited in claim ~~33~~ <u>32</u>,

2   wherein each critical field k of the ~~document~~ <u>check</u>, in addition to being

3   covered by encrypted versions of X, $\text{Sign}_{k,0}(X)$, is covered with another

4   encrypted version of X, $\text{Sign}_k(X)$, where $\text{Sign}_k(X)$ is another cryptographic

5   function or family thereof different from the cryptographic function

6      $\text{Sign}_{k,0}(X)$ which is known to a larger number of authorized banks and

7   institutions for performing an initial authentication of the check.

1   35 (Currently Amended). The ~~document~~ check recited in claim 34, wherein

2   each critical field k of the ~~document~~ check, in addition to being covered by

3   encrypted versions of X, $\text{Sign}_{k,0}(X)$ and $\text{Sign}_k(X)$, is covered with a third

4   encrypted version of X, $\text{Sec}_k(X)$ is another cryptographic function or

5   family thereof different from the cryptographic functions $\text{Sign}_{k,0}(X)$ and

6      $\text{Sign}_k(X)$ which is known to a small group within the bank or institution

7   which issues the check for performing final authentication of the check.

1   36 (Currently Amended). The ~~document~~ check recited in claim 35, wherein

2   the encrypted function $\text{Sign}_k(X)$ ~~are~~ is communicated to banks and other

3   authorized institutions involved in depositing checks and the encrypted

4   function $\text{Sign}_k(X)$ allows the payee's bank to perform a first authentication

5   of the check.

1   37 (Currently Amended). The ~~document~~ check recited in claim 36, wherein

2   key $\text{Sign}_{k,0}$ remains the exclusive property of the issuing bank and the

3   encrypted function $\text{Sign}_{k,0}(X)$ is used exclusively by the issuing bank and

4   branches involved in the clearing of checks.

1   38 (Currently Amended). The ~~document~~ check recited in claim 37, wherein

2   secret key Sec_k is exclusively known to the issuing bank and the encrypted

3   function $\text{Sec}_k(X)$ is used by the issuing bank as a final instrument to verify

4   the check.

1   39 (New). An apparatus for protecting a check, which will be transformed

2   into a value bearing instrument after adding additional markings to the

3 check, from fraudulent alteration of the markings comprising:

4 printing means for printing checks having printed thereon a unique

5 identifier X, the unique identifier including a bank ID, an account ID

6 number and a check number, the check further having critical fields k,

7 k=1,2,3..., the critical fields including a date field, a payee field, amount

8 fields, a payer's field, and an endorser's field, and each critical field k,

9 k=1,2,3..., being covered a large number of lines of fine print comprising

10 encrypted versions α the unique identifier X printed on the document,

11 $Sign_{k,0}(X)$, where $Sign_{k,0}(X)$ is a cryptographic function or family thereof

12 which is known only to an institution which issues the document;

13 digitizing means for generating a digitized version of the check in

14 at least selected locations where markings are added to transform the check

15 into a value bearing instrument;

16 first extracting means for extracting from the digitized version of

17 the document the unique identifier X and a corresponding digital

18 encryption of X, $Sign_k(X)$, which is known to a large number of authorized

19 institutions; and

20 first comparing means for comparing a decrypted version of

21 $Sign_k(X)$ to the unique identifier X as an initial authentication of the

22 document.

1 40 (New). The apparatus recited in claim 39, wherein each critical field of

2 the check, in addition to being covered by the encrypted version of X,

3 $Sign_{k,0}(X)$, is covered by another encrypted version of X, $Sign_k(X)$, where

4 $Sign_{k,0}(X)$ being used to authenticate the document, $Sign_k(X)$, where

5 $Sign_k(X)$ is another cryptographic function or family thereof different from

6 the cryptographic function $Sign_{k,0}(X)$ which is known to a larger number of

7 authorized institutions for performing an initial authentication of the

8 check, further comprising:

9 second extracting means for extracting from the digitized version

10 of the document the unique identifier X and the corresponding digital

11 encryption of X, $Sign_{k,0}(X)$, which is known only to an institution that

12   issues the document; and

13   second comparing means for comparing a decrypted version of

14      $Sign_{k,0}(X)$ to the unique identifier X as a further authentication of the

15   document.

1   41 (New). The apparatus of claim 40, wherein each critical field k of the

2   check, in addition to being covered by the encrypted versions of X,

3      $Sign_{k,0}(X)$ and $Sign_k(X)$, is covered with another encrypted version of X,

4   and $Sec_k(X)$, where $Sec_k(X)$ is another cryptographic function or family

5   thereof different from the cryptographic functions $Sign_{k,0}(X)$ and $Sign_k(X)$

6   and which is known to a small group within the institution which issues

7   the document for performing final authentication of the check, further

8   comprising:

9   third extracting means for extracting from the digitized version of

10   the document the unique identifier X and a corresponding digital

11   encryption of X, $Sec_k(X)$, which is known to a small group within the

12   institution that issues the document; and

13   third comparing means for comparing a decrypted version of

14      $Sec_k(X)$ to the unique identifier X as a final authentication of the

15   document.

1   42 (New). The apparatus of 41, wherein the cryptographic functions $Sign_k$,

2      $Sign_{k,0}$ and Sec_k, are indexed by a number corresponding to the field k, so

3   that each line comprises different encryptions of X such that each

4   cryptographic functions $Sign_k(X)$, $Sign_{k,0}(X)$ and $Sec_k(X)$ are families of

5   different cryptographic functions, wherein the families of cryptographic

6   functions $Sign_k$, $Sign_{k,0}$ and Sec_k prevent cryptographic functions which

7   have been obscured at different places by marks added to the check from

8   being used to reconstitute the full cryptographic function.

1   43 (New). The apparatus recited in claim 41, further comprising one or

2   more secure cryptographic generators (SCGs) for computing the first

3 family of encrypted functions $Sign_k(X)$, the second family of encrypted

4 functions $Sign_{k,0}(X)$, and the third family of encrypted functions $Sec_k(X)$.

5 44 (New). The apparatus recited in claim 39, further comprising a database

6 where the unique identifier X and first encrypted function $Sign_k(X)$ is

7 registered, said database being accessed by the payee's bank to determine

8 whether the check has been previously presented for deposit.